



Terms of Personal Data Processing in the Context of Receiving and Investigating Reports

(hereinafter “DIAS” or the “Company”) hereby informs that it complies with the applicable legal framework on the protection of personal data and in particular with the General Data Protection Regulation (EU) 2016/679 (GDPR). This document is issued in compliance with the provisions of the Company’s Personal Data Protection Policy.

The Company maintains an internal communication channel (through a designated person, the Whistleblowing Officer - “W.O.”) for employees, partners, and third parties, in order for these persons to be able to submit reports of incidents that come to their attention and concern violations of applicable legislation, the Code of Ethics and Conduct, and the Company’s Policies, as further specified in the Whistleblowing Management Policy. In this context, the Company may collect and process the following categories of personal data concerning persons submitting a report and/or persons to whom the report refers or who are involved in the reported incidents:

- Personal details (full name, contact details)
- Relationship with the Company
- Place and time of submission of the report
- Category of violation
- Information, incidents and documents supporting / evidencing the violation
- Assessment of the report
- Disciplinary or other sanctions that may be imposed

The legal basis for this processing is, on the one hand, compliance with the Company’s legal obligations (where the report concerns incidents provided for by law, in particular Law 4990/2022 and Law 4808/2021, as in force from time to time – Art. 6(1)(c) GDPR), and on the other hand, the pursuit of the Company’s legitimate interests (where the report concerns incidents not explicitly provided for by law – Art. 6(1)(f) GDPR). The Company’s legitimate interest lies in the prevention and suppression of misconduct that may jeopardize its reputation, financial performance, and/or existence.

In any case, the purpose of processing is exclusively the investigation and assessment of the reported incidents, in order to impose disciplinary measures where applicable, protect the interests of employees and the Company, and suppress unlawful or unethical business practices.

The Company processes the personal data it collects and retains as Data Controller in accordance with the procedure set out in the Whistleblowing Management Policy and applicable law. The Company does not carry out automated decision-making.

Retention Period of Data

The Company retains personal data for five (5) years from the submission of the report. In cases where criminal offences amounting to felonies are reported, the Company retains such reports until the statute of limitations expires. The retention period may be extended in the event of proceedings before courts or other competent public authorities.

In addition, the Company immediately deletes, without further notice, data that are manifestly unrelated to the submitted report and/or reports that are unfounded, abusive, or do not contain incidents constituting a violation, as provided in the Whistleblowing Management Policy.

Recipients of the Data



In order to achieve the purpose of processing, the Company may disclose data to third parties (processors, independent advisors), who are bound to maintain an adequate level of data protection and to implement appropriate technical and organizational measures for data security.

The Company may also disclose data to judicial or other competent public authorities, upon request or ex officio to comply with its legal obligations.

In case of transfers of data outside the EU, the Company ensures the implementation of appropriate safeguards under applicable legislation. Further information may be requested from the DPO (see below).

Data Subject Rights

Data subjects have the following rights in relation to their personal data:

- Right of access
- Right to rectification and/or updating
- Right to data portability
- Right to erasure
- Right to restriction of processing and objection
- Right to withdraw consent, where consent is the legal basis for processing

These rights are exercised subject to the conditions and limitations of applicable whistleblowing legislation and the GDPR, by submitting a relevant request to the Company and/or the Data Protection Officer.

Requests may be submitted via the completed Data Subject Rights Request Form (Annex I) to dpo@dias.com.gr, by post to the Company's address marked for the attention of the Data Protection Officer, or by any other appropriate means.

Data subjects also retain the right to lodge a complaint with the Hellenic Data Protection Authority (1-3 Kifisias St., 115 23 Athens – Tel: +30 210 6475600 – Email: contact@dpa.gr).

The Company responds to requests within thirty (30) days of receipt. This period may be extended by an additional sixty (60) days, with prior notification explaining the reasons for the delay.

The Company makes every reasonable effort to process personal data lawfully, fairly, and securely. If a data subject believes that their personal data may have been violated, they may contact the Company via email at dpo@dias.com.gr, by post, or by any other appropriate means.

Security – Confidentiality

The Company has implemented appropriate technical and organizational measures to ensure the highest possible level of data protection in accordance with legal principles. It has also developed and implements an integrated Information Security and Business Continuity Management System, compliant with PCI DSS, ISO 27001, and ISO 22301 standards.

Data Protection Officer (DPO)

For any information regarding the processing of your personal data by DIAS and the exercise of your legal rights, you may contact the Data Protection Officer:



Email: dpo@dias.com.gr

Tel: +30 210 6171713

Address: 2 Alamanas Street, Marousi, 15125, GreeceE

Controller Identity

The company under the name INTERBANKING SYSTEMS S.A. ("DIAS S.A."), headquartered in Marousi, Attica, 2 Alamanas Street, 15125, Greece, Tel: +30 210 6171600, Email: info@dias.com.gr, General Commercial Registry No. 000740401000.

ANNEX I – DATA SUBJECT RIGHTS REQUEST FORM

To: INTERBANKING SYSTEMS S.A.

Date: _____

APPLICANT DETAILS:
Full Name:
Address:
Contact details (landline/mobile/email):
Relationship with the Company:
Additional information:

I hereby request to exercise my right to:

- ☐ Access personal data
- ☐ Rectification / supplementation / updating of personal data
- ☐ Restriction of processing
- ☐ Data portability
- ☐ Erasure of personal data
- ☐ Objection to processing
- ☐ Withdrawal of consent

Detailed description of request:

I request that communication with DIAS and receipt of my request be made:

- ☐ By email (please specify email address)
- ☐ By post (please specify full address)



☐ By other means (please specify)

I solemnly declare that all information provided in this application is true and accurate.

INFORMATION ON PERSONAL DATA

DIAS processes your request in accordance with applicable law and its Personal Data Protection Policy published on its website. If additional information is required, the Company may request further details. Applications are retained for 12 months from receipt. Personal data provided through this form are processed for the purpose of handling your request and for other lawful purposes as described in the Company's Policy and applicable law. You retain your rights of access, rectification, erasure, restriction, objection, and complaint to the Hellenic Data Protection Authority.

For further information, you may contact the DPO (dpo@dias.com.gr, +30 210 6171600 / 210 6171713, 2 Alamanas Street, Marousi, 15125, Greece).

Applicant

(Signature)

Disclaimer: This is an English translation of the official company text originally drafted in Greek, provided for informational purposes only. In the event of any discrepancy between the Greek and the English versions, the Greek version shall prevail.